

REMARKS

No claims have been amended. Claims 1-31 are pending in this application.

Claims 1-31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Kara (US 6,297,891) in view of Ulvr et al. (US 6,398,106). Reconsideration is respectfully requested.

The present invention is directed to a mail piece verification system for processing a mail piece that includes an incoming mail processing center for receiving a mail piece and obtaining data from the mail piece. The mail piece data is uploaded to a data center that performs a verification check on the mail piece data and downloads instructions, based upon the verification check, to an outgoing mail processing center located downstream from the incoming mail processing center. The outgoing mail processing center then uses the instructions, received from the data center, to process the mail piece.

In view of the above, claim 1 is directed to a mail piece verification system for processing mail pieces that comprises “an incoming mail processing center for receiving the mail piece and obtaining the mail piece data, the incoming mail processing center including a plurality of mail processing machines that perform automated processing of mail pieces; an outgoing mail processing center located downstream in the path of travel from the incoming mail processing center, the outgoing mail processing center including a plurality of mail processing machines that perform automated processing of mail pieces; and a data center in operative communication with the incoming mail processing center and the outgoing mail processing center” wherein “the incoming mail processing center uploads the mail piece data to the data center; the data center performs a verification check on the mail piece data and downloads instructions based upon the verification check to the outgoing mail processing center; and the outgoing mail processing center uses the instructions to control operation of at least one of the mail processing machines located at the outgoing mail processing center to process the mail piece.”

Kara is directed to a system and method that provides for the certification of electronic delivery of a transmitted document. The certified transmission of a document is

accomplished by transmitting the document from a sending site, through a certification system, to a recipient site. A user invokes a first processor based system (PC) to certifiably transmit a selected document via a program, referred to as the "Send" program, stored on the first PC. The Send program requests input from the user, co-existing process, or coupled devices, about the electronic document to be transmitted, to whom it is to be transmitted, including an electronic address such as e-mail address or telephone number of receiving data communications equipment, level of certification desired, etc. The Send program may encrypt the selected electronic document for transmission. Upon encryption, a cipher, comprised of selected data bits, is generated by the Send program. This cipher includes a checksum and/or total bit count of the encrypted electronic message and additional information provided by the Send program such as the recipient's electronic address identification of the sending site, time of document transmission, and number of pages in the document to be transmitted. The encrypted electronic document and associated cipher are transmitted by the Send program to a remote certification device, itself a second PC. The remote certification device stores a program (the "Certification" program), which receives encrypted electronic documents and associated ciphers from sending sites and verifies the received encrypted document against the cipher. Upon verification of the received encrypted document, the Certification program transmits both the encrypted document and the cipher to the recipient indicated by the cipher. The recipient site is also a PC. The recipient site stores a program (the "Receive" program), which receives encrypted electronic documents and associated ciphers from certification systems and verifies the received encrypted document against the cipher. Upon verification, a cipher is generated by the Receive program. This cipher includes a checksum of the received encrypted electronic document and additional information provided by the Receive program, such as the exact time of receipt and identification of recipient site. The cipher is transmitted to the certification system. The Certification program verifies that the checksum of the encrypted electronic document received by the Receive program matches the checksum of the encrypted electronic document originally sent by the Send program. Upon a match, the Certification program generates an indicia of certification which includes the checksum of the encrypted electronic document, date and time of receipt by the recipient, number of pages in the document, identification of the recipient, and identification of the sender. This indicia is then transmitted to the sender for proof of certified transmission of an electronic document.

The certification indicia, along with the private key, is transmitted to the recipient. The Receive program then utilizes the private key to decrypt the received encrypted electronic document. Upon decryption, the Receive program integrates the certification indicia within the decrypted document for subsequent printing. (Col. 4, line 47 to Col. 5, line 49).

Note first that Kara is in no way directed to the verification of mail pieces, i.e., determining if an indicium on a mail piece that evidences payment of postage for the mail piece is valid. Kara is instead directed to a system for transmitting electronic documents that can establish the time a transmission was sent, proving where it was sent from, and proving the exact content of the transmission to a high degree of certainty. (Col. 1, lines 59-63). There is no disclosure, teaching or suggestion in Kara of a mail piece verification system for processing a mail piece in a path of travel that comprises an incoming mail processing center for receiving the mail piece and obtaining mail piece data, an outgoing mail processing center located downstream in a path of travel from the incoming mail processing center, and a data center in operative communication with the incoming mail processing center and the outgoing mail processing center, wherein the incoming mail processing center uploads the mail piece data to the data center, the data center performs a verification check on the mail piece data and downloads instructions based upon the verification check to the outgoing mail processing center, and the outgoing mail processing center used the instructions to control operation of at least one mail processing machine located at the outgoing mail processing center to process the mail piece as in the present invention.

The Office Action contends that Kara, at Col. 2, line 21 to Col. 3, line 35, discloses these features. The passage cited in the Office Action is reproduced, in its entirety, below.

The difference in each indicia at each receiving location is due to the unique characteristics of that station as contained in the indicia. In this manner, the authenticity of each transmission can be determined by comparison of the received bits to the code of the receiving station. Since included in each transmission is the exact time of the reception, and the exact number of received bits, the probability of two transmissions having the same cipher is very remote indeed.

Part of the printed indicia is an encrypted checksum for the document, or each page if desired. In one embodiment, the printed indicia will appear only on the first page of the printed transmitted document, with the checksum for all of the pages encrypted onto this single printed indicia. In a more precise system, and an alternative embodiment, each received page printed is provided with its own indicia, having contained therein a count of bits for that page as well as other information unique to that page. Additionally, the recipient of the document could, if desired, select between the two systems depending upon the level of authentication desired.

In other embodiments, the transfer of the electronic document is accomplished through a system independent from either end of the transmission. The independent system may be utilized for a higher level of authentication or certification as well as additional services. In one embodiment, the independent system provides a high degree of certification by verifying the transmission and receipt of the electronic document from the sending end to the receiving end. Verification by the independent system involves checking data bits associated with the document sent from the sending end against data bits associated with the document received by the receiving end. These data bits may include a special version of the sender's and/or recipient's station code, the number of pages, the time, the total bit count of the document transmission, and other data associated with the document and its transmission. It shall be appreciated that an advantage of such an embodiment is realized in the fact that the document may be directly transmitted by the sender to the receiver with only the verification data bits being communicated to the independent system. Upon verification, the independent system transmits an indicia of certification to the receiving end to be included in the printed document as well as to the sending end for proof of certified delivery.

In another embodiment, the independent system receives the document from the sending end and relays it to the receiving end. Both the receiving and sending of the document by the independent system involve verification of the document's contents against data bits associated with the document's transmission. These data bits correspond to a special version of the sender's or recipient's station code, the number of pages, the time, the total bit count of the document transmission, or other data associated with the document and its transmission. Upon verification of receipt of the document by the receiving

end, the independent system issues an indicia of certification to the receiving end to be included in the printed document as well as to the sending end for proof of certified delivery.

An advantage of the utilization of the independent system in the above manner is that any sender's certification indicia can be later authenticated with a duplicate indicia stored within the independent system. Moreover, the transmission of the electronic document through an independent system provides an opportunity for additional services at the independent system. In one embodiment, the independent system provides document archiving services for documents transmitted there through.

The foregoing has outlined rather broadly the features and technical advantages of the present invention in order that the detailed description of the invention that follows may be better understood. Additional features and advantages of the invention will be described hereinafter which form the subject of the claims of the invention. It should be appreciated by those skilled in the art that the conception and the specific embodiment disclosed may be readily utilized as a basis for modifying or designing other structures for carrying out the same purposes of the present invention. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims..

It is unclear to Applicants where each of the features as recited in the claims of the present invention can be found in the above passage from Kara, and respectfully request the Examiner to provide support for this contention. The system of Kara is not related in any manner to the verification of mail pieces, nor does Kara include any type of incoming mail processing centers, outgoing mail processing centers or a data center in communication therewith. Furthermore, there is no disclosure, teaching or suggestion anywhere in Kara of an incoming mail processing center uploading mail piece data to a data center, the data center performing a verification check on the mail piece data and downloading instructions based upon the verification check to the outgoing mail processing center. There is also no disclosure, teaching or suggestion in Kara of the outgoing mail processing center using the

instructions from the data center to control operation of a mail processing machine to process the mail piece.

The reference to Ulvr et al. does not cure the above deficiencies. There is no disclosure, teaching or suggestion in Ulver et al. of a mail piece verification system for processing mail piece that comprises an outgoing mail processing center located downstream in the path of travel from the incoming mail processing center, the outgoing mail processing center including a plurality of mail processing machines that perform automated processing of mail pieces; and a data center in operative communication with the incoming mail processing center and the outgoing mail processing center wherein the incoming mail processing center uploads the mail piece data to the data center; the data center performs a verification check on the mail piece data and downloads instructions based upon the verification check to the outgoing mail processing center; and the outgoing mail processing center uses the instructions to control operation of at least one of the mail processing machines located at the outgoing mail processing center to process the mail piece as is recited in claim 1.

For at least the above reasons, Applicants respectfully submit that claim 1 is allowable over the prior art of record. Claims 2-14, dependent upon claim 1, are allowable along with claim 1 and on their own merits.

Claim 15 includes limitations substantially similar to those of claim 1. For the same reasons claim 1 is allowable over the prior art of record, Applicants respectfully submit that claim 15 is allowable over the prior art of record. Claims 16-26, dependent upon claim 15, are allowable along with claim 15 and on their own merits.

Claim 27 includes limitations substantially similar to those of claim 1. For the same reasons claim 1 is allowable over the prior art of record, Applicants respectfully submit that claim 27 is allowable over the prior art of record. Claims 28-31, dependent upon claim 27, are allowable along with claim 27 and on their own merits.

In view of the foregoing remarks, it is respectfully submitted that the claims of this case are in a condition for allowance and favorable action thereon is requested.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Brian A. Lemm", is written over a horizontal line.

Brian A. Lemm
Reg. No. 43,748
Attorney for Applicants
Telephone (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000